Exam : 312-38

Title : Certified Network Defender

https://www.passcert.com/312-38.html

1.Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

A. Mitigation

B. Assessment

C. Remediation

D. Verification

Answer: C

2.How is application whitelisting different from application blacklisting?

A. It allows all applications other than the undesirable applications

B. It allows execution of trusted applications in a unified environment

C. It allows execution of untrusted applications in an isolated environment

D. It rejects all applications other than the allowed applications

Answer: D

3.John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router.

Which command will John use to enable NetFlow on an interface?

A. Router(Config-if) # IP route - cache flow

B. Router# Netmon enable

C. Router IP route

D. Router# netflow enable

Answer: A

4.Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes though the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the __________implementation of a VPN.

A. Full Mesh Mode

B. Point-to-Point Mode

C. Transport Mode

D. Tunnel Mode

Answer: D

5.Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled.

Which of the following command allows Sophie to do so?

A. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol

B. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol

D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

Answer: B

6.Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic.
What type of scan is Cindy attempting here?
A. The type of scan she is usinq is called a NULL scan.
B. Cindy is using a half-open scan to find live hosts on her network.
C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
D. She is utilizing a RST scan to find live hosts that are listening on her network.
Answer: B

7.Which of the following helps prevent executing untrusted or untested programs or code from untrusted or unverified third-parties?
A. Application sandboxing
B. Deployment of WAFS
C. Application whitelisting
D. Application blacklisting
Answer: A

8.A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines.
What are the other f unction(s) of the device? (Select all that apply)
A. Provides access memory, achieving high efficiency
B. Assigns user addresses
C. Enables input/output (I/O) operations
D. Manages security keys
Answer: B,C,D

9.Damian is the chief security officer of Enigma Electronics. To block intruders and prevent any environmental accidents, he needs to set a two-factor authenticated keypad lock at the entrance, rig a fire suppression system, and link any video cameras at various corridors to view the feeds in the surveillance room.
What layer of network defense-in-depth strategy is he trying to follow?
A. Physical
B. Perimeter
C. Policies and procedures
D. Host
Answer: A

10.John wants to implement a packet filtering firewall in his organization's network.
What TCP/IP layer does a packet filtering firewall work on?
A. Application layer

B. Network Interface layer
C. TCP layer
D. IP layer
Answer: D

11.Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the------------------------- authentication technique to satisfy the management request.
A. Two-factor Authentication
B. Smart Card Authentication
C. Single-sign-on
D. Biometric
Answer: C

12.Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an _______ for legal advice to defend them against this allegation.
A. Evidence Manager
B. Incident Handler
C. Attorney
D. PR Specialist
Answer: C

13.The risk assessment team in Southern California has estimated that the probability of an incident that has potential to impact almost 80% of the bank's business is very high.
How should this risk be categorized in the risk matrix?
A. High
B. Medium
C. Extreme
D. Low
Answer: C

14.Michael decides to view the-----------------to track employee actions on the organization's network.
A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set
Answer: B